

High-dimensional Quantum Key Distribution with Photonic Orbital Angular Momentum

Mohammad Mirhosseini^{1,*}, Omar S. Magaña-Loaiza¹, Malcolm N. O'Sullivan¹,
Brandon Rodenburg¹, Mehul Malik^{1,2}, Martin P. J. Lavery³, Miles J. Padgett³,
Daniel J. Gauthier⁴, and Robert W. Boyd^{1,5,3}

¹The Institute of Optics, University of Rochester, Rochester, New York 14627, USA

²Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmannngasse 3,
A-1090 Vienna, Austria

³School of Physics and Astronomy, University of Glasgow, Glasgow, G12 8QQ, UK

⁴Department of Physics, Duke University, Durham, NC 27708 USA

⁵Department of Physics, University of Ottawa, Ottawa ON K1N 6N5, Canada

*mirhosse@optics.rochester.edu

Abstract: We experimentally demonstrate a quantum cryptography system based on photonic orbital angular momentum. The system achieves a channel capacity of 2.1 bits per sifted photon through the use of a 7-dimensional alphabet for encoding information.

© 2014 Optical Society of America

OCIS codes: 270.0270, 270.5568, 270.5585.

Quantum key distribution (QKD) is a protocol for secure distribution of a secret key between two parties [1]. Any attempts made by a third party, traditionally known as Eve, to eavesdrop inevitably leads to errors that can be detected by the legitimate parties Alice and Bob due to a fundamental property of quantum physics known as the no-cloning theorem [2]. QKD schemes till date have relied on polarization of a photon for encoding information [3].

Recently, photonic orbital angular momentum (OAM) has been identified as an extremely useful resource for transferring information [4, 5]. The discrete unbounded state space of OAM provides a test bed for realizing multilevel quantum states (qudits) [6]. Employing multi-level states in a QKD protocol provides additional robustness against eavesdropping as well as enhancement in the key generation rate [7].

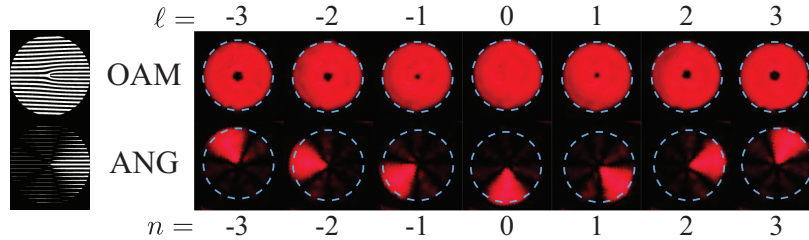


Fig. 1. The set of 7 OAM modes used for information encoding (top). The ANG modes are used as mutually unbiased set with respect to the OAM basis (bottom). Examples of the computer generated holograms for creating OAM and ANG modes (left).

Here we describe an experimental scheme for performing multi-level quantum cryptography with OAM modes. Similar to the BB84 protocol, Alice randomly chooses her photons from two mutually unbiased high-dimensional bases (MUBs) in a prepare-and-measure scheme (See Fig. 1). The primary encoding basis is the 7-dimensional set of OAM modes $\Psi_{\text{OAM}}^{\ell} = e^{i\ell\phi}$, with $\ell \in \{-3 : 3\}$. We construct the mutually unbiased basis of azimuthal angle (ANG) using a linear combination of OAM modes of index $|\ell| \leq 3$ with equal weights

$$\Psi_{\text{ANG}}^n = \frac{1}{\sqrt{d}} \sum_{\ell=-N}^N \Psi_{\text{OAM}}^{\ell} \exp\left(\frac{i2\pi n\ell}{d}\right). \quad (1)$$

The modes are generated by modifying the width and position parameters of a binary grating realized on a digital micro-mirror device (DMD) [8]. The DMD used in the setup provides the ability to rapidly switch among the modes

at a speed of 4 kHz, in contrast to phase-only spatial light modulators (SLMs) which are limited to a frame rate of 60 Hz. Alice sends each symbol by illuminating the computer generated holograms with 125 ns pulses that contains $\mu = 0.1$ photons on average (See Fig. 2).

Using a combination of a coordinate transformation and a beam-copying technique, the OAM and ANG modes are sorted to an array of localized spots with a separation efficiency of 93% [9, 10]. Error correction and privacy amplification is performed via a classical link realized by an ethernet cable running the TCP/IP protocol once Alice and Bob have collected a sufficiently long raw key. The mutual information between Alice and Bob is calculated from the data as 2.1 bits per sifted photon. This is more than twice the maximum allowable capacity of a two-dimensional QKD system. The QBER of our scheme is measured to be 10.5%, which is sufficient for proving unconditional security against coherent and individual eavesdropping attacks for a sufficiently long key.

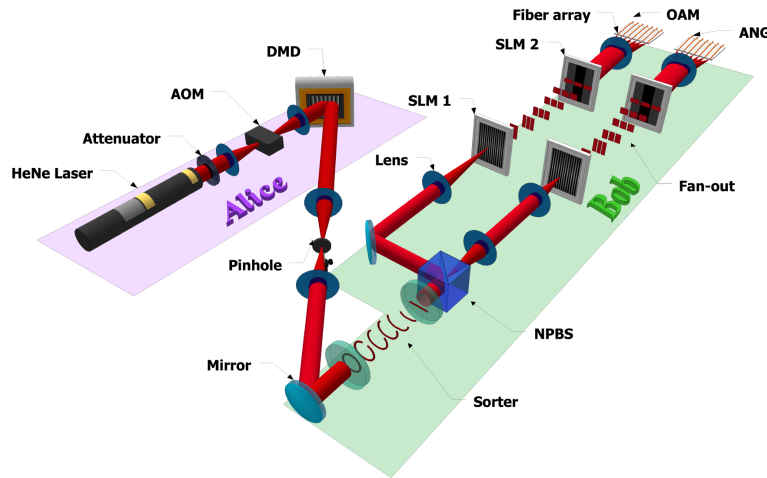


Fig. 2. Schematic diagram of the experimental setup.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in "Proc. IEEE Int. Conf.," (Bangalore, 1984), pp. 175–179.
2. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, 802–803 (1982).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–195 (2002).
4. J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," *Nature Photonics* **6**, 488–496 (2012).
5. G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, "Free-space information transfer using light beams carrying orbital angular momentum," *Optics Express* **12**, 5448–5456 (2004).
6. A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons," *Nature* **412**, 313–316 (2001).
7. N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of Quantum Key Distribution Using d-Level Systems," *Physical Review Letters* **88**, 127,902 (2002).
8. M. Mirhosseini, O. S. Magaña-Loaiza, C. Chen, B. Rodenburg, M. Malik, and R. W. Boyd, "Rapid generation of light beams carrying orbital angular momentum," *Optics Express* **21**, 30,196–30,203 (2013).
9. M. P. J. Lavery, D. J. Robertson, G. C. G. Berkhout, G. D. Love, M. J. Padgett, and J. Courtial, "Refractive elements for the measurement of the orbital angular momentum of a single photon," *Optics Express* **20**, 2110 (2012).
10. M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, "Efficient separation of the orbital angular momentum eigenstates of light," *Nature Communications* **4**, 2781 (2013).